邮件安全设备的DANE

目录

简介

本文档介绍ESA出站邮件流的DANE实施。

先决条件

ESA概念和配置的一般知识。

实施DANE的要求：

- 支持DNSSEC的DNS解析器
- 采用AsyncOS 12.0或更高版本的ESA

背景信息

DANE已引入ESA 12以进行出站邮件验证。

基于DNS的命名实体身份验证(DANE)。

- DANE是一种互联网安全协议，允许X.509数字证书使用DNSSEC绑定到域名。(RFC 6698)
- DNSSEC是IETF规范的集合，用于通过使用公钥加密保护DNS记录。(非常简单的解释。RFC 4033、RFC 4034和RFC 4035)

实施注意事项

验证ESA是否使用支持dnssec的DNS解析器。

要实施DANE，需要DNS功能来执行DNSSEC/DANE查询。

要测试ESA DNS DANE功能，可以从ESA CLI登录执行简单测试。

CLI命令“daneverify”将执行复杂查询以验证域是否能通过DANE验证。

同一命令可与已知正常的域一起使用，以确认ESA能否解析dnssec查询。

“ietf.org”是全球公认的来源。执行cli命令“daneverify”将验证DNS解析器是否支持DANE。

有效通过：支持DANE的DNS服务器“DANE成功”结果IETF.org

```
> daneverify ietf.org

SECURE MX record(mail.ietf.org) found for ietf.org
SECURE A record (4.31.198.44) found for MX(mail.ietf.org) in ietf.org
Connecting to 4.31.198.44 on port 25.
Connected to 4.31.198.44 from interface 216.71.133.161.
SECURE TLSA record found for MX(mail.ietf.org) in ietf.org
Checking TLS connection.
TLS connection established: protocol TLSv1.2, cipher ECDHE-RSA-AES256-GCM-SHA384.
Certificate verification successful
TLS connection succeeded ietf.org.
DANE SUCCESS for ietf.org
DANE verification completed.
```

无效失败：IETF.org的非DANE CAPABLE DNS服务器“BOGUS”结果

```
> daneverify ietf.org

BOGUS MX record found for ietf.org
DANE FAILED for ietf.org
DANE verification completed.
```

有效失败：daneverify cisco.com > cisco尚未实施DANE。这是支持dnssec的解析器的预期结果。

```
> daneverify cisco.com

INSECURE MX record(alln-mx-01.cisco.com) found for cisco.com
INSECURE MX record(alln-mx-01.cisco.com) found. The command will still proceed.
INSECURE A record (173.37.147.230) found for MX(alln-mx-01.cisco.com) in cisco.com
Trying next MX record in cisco.com
INSECURE MX record(rcdn-mx-01.cisco.com) found for cisco.com
INSECURE MX record(rcdn-mx-01.cisco.com) found. The command will still proceed.
INSECURE A record (72.163.7.166) found for MX(rcdn-mx-01.cisco.com) in cisco.com
Trying next MX record in cisco.com
INSECURE MX record(aer-mx-01.cisco.com) found for cisco.com
INSECURE MX record(aer-mx-01.cisco.com) found. The command will still proceed.
INSECURE A record (173.38.212.150) found for MX(aer-mx-01.cisco.com) in cisco.com
DANE FAILED for cisco.com
DANE verification completed.
```

如果上述测试“有效”工作：

- 谨慎的做法是在为域添加配置文件之前测试每个域。
- 更积极的方法是在默认目标控制配置文件上配置DANE，并查看谁通过/失败。

邮件方向确定DANE是否将进行验证。

配置了“中继”操作的发件人组/邮件流策略将执行DANE验证。

配置了“接受”操作的发件人组/邮件流策略将不执行DANE验证。

> **警告：**如果ESA在默认策略上启用目标控制“DANE”**，则存在交付失败的风险。** 如果内部拥有的域（如RAT中列出的域）同时通过RELAY和ACCEPT邮件流策略，并且域存在SMTP路由。

SMTP路由

除非将“目标主机”配置为“USEDNS”，否则DANE在SMTP路由上将失败。

DANE Osprotic不会传送邮件，在退回配置文件计时器到期之前，邮件将包含在“传送队列”中。

为什么？DANE验证被跳过，因为SMTP路由是对真目标的修改，可能无法正确使用DNS。

解决方案：创建目标控制配置文件以明确禁用包含SMTP路由的域的DANE验证

DANE机会或DANE必备

在DANE验证期间执行以下查找。

每个验证会馈送内容以执行后续验证。

- MX记录查找验证是否>>安全、不安全、伪造
- 记录查找验证是否>>安全不安全>伪造
- TLSA记录查找验证是否>>安全、不安全、伪造、NXDOMAIN
- 证书验证>>成功，失败

安全：

- DNS验证了是否存在包含RRSIG验证的签名RRSIG DS和DNSKEY的安全记录（在信任链上）。

不安全：

- DNS确定域没有启用DNSsec的记录。

假的：

- 不完整，但存在dnssec条目可能无法通过验证。
- 由于密钥过期，记录无效。
- 信任链中缺少记录或密钥。

NXDOMAIN

- 在DNS中找不到记录。

上述记录检查和验证结果的组合将确定“DANE成功” | DANE失败 | DANE回退到TLS。"

例如：如果没有为example.com的MX记录发送RRSIG，则检查父区域(.com)以查看example.com是否具有DNSKEY记录，指示example.com应对其记录进行签名。此验证继续进行信任完成，根区域(.)密钥验证已到达，根区域的密钥与ESA期望的匹配（ESA上的硬编码值，根据RFC5011自动更新）。

DANE必填

MX RECORD	A RECORD	TLSA	CERTIFICATE Verify	ACTION
Secure	Secure	Secure	Success	DANE Success
Secure	Secure	Secure	Failed	DANE Fail
Secure	Secure	Insecure		DANE Fail
Secure	secure	NXDOMAIN		DANE Fail
Secure	Secure	Bogus		DANE Fail
Secure	Insecure			DANE Fail
secure	Bogus			DANE Fail
Insecure	Secure	Secure	Success	DANE Fail
Insecure	Secure	Secure	Fail	DANE Fail
Insecure	Secure	Insecure		DANE Fail
Insecure	Secure	NXDOMAIN		DANE Fail
Insecure	Secure	Bogus		DANE Fail
Insecure	Insecure			DANE Fail
Insecure	Bogus			DANE Fail
Bogus				DANE Fail

Mail will not be delivered for the messages in the box

DANE必填

> **注意：**DANE OSPRICTIC**不像TLS PREFERRED那样行为。**下表的ACTION部分会导致DANE FAIL，不会为Mandatory或Ospritic提供。邮件将保留在传送队列中，直到计时器到期，然后传送终止。

DANE机会主义

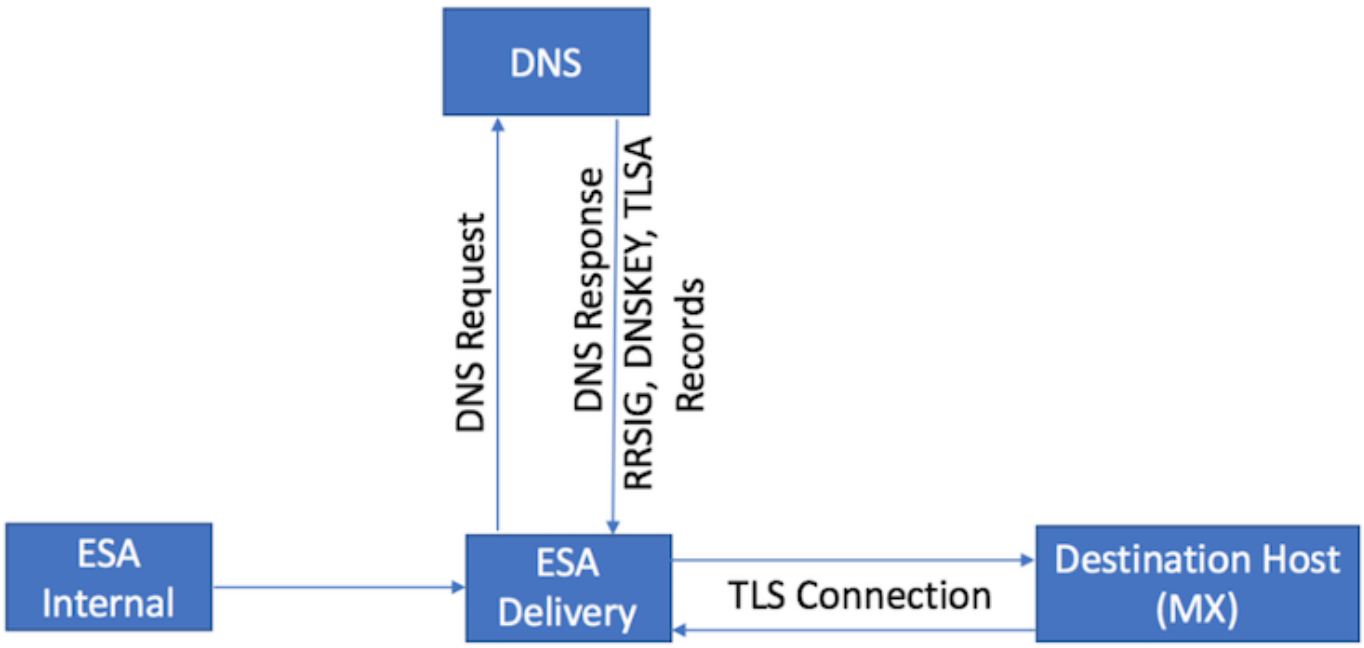
MX RECORD	A RECORD	TLSA	CERTIFICATE Verify	ACTION
Secure	Secure	Secure	Success	DANE Success
Secure	Secure	Secure	Failed →	DANE Fail
Secure	Secure	Insecure		Fallback to opportunistic TLS flow
Secure	secure	NXDOMAIN		Fallback to opportunisticTLS flow
Secure	Secure	Bogus	→	DANE Fail
Secure	Insecure	Mail will not be delivered for the marked arrows		Fallback to opportunistic TLS flow
secure	Bogus		→	DANE Fail
Insecure	Secure	Secure		Fallback to opportunisticTLS flow
Insecure	Secure	Insecure		Fallback to opportunisticTLS flow
Insecure	Secure	NXDOMAIN		Fallback to opportunisticTLS flow
Insecure	Secure	Bogus	→	DANE Fail
Insecure	Insecure			Fallback to opportunisticTLS flow
Insecure	Bogus			DANE Fail
Bogus			→	DANE Fail

DANE机会主义

在多个设备环境上启用DANE

下图说明在多设备环境中启用DANE时的工作流程。

如果环境有多个ESA设备层，一个用于扫描，另一个用于传送消息确保DANE仅在直接连接到外部目标的设备上配置。



多ESA设计。在交付ESA上配置的DANE

管理多个DNS解析器

如果ESA配置了多个DNS解析器，其中一些支持DNSSEC，另一些不支持DNSSEC，思科建议使用更高的优先级（较低的数值）配置支持DNSSEC的解析器，以防止不一致。

这会阻止支持DANE的非DNSSEC解析程序将支持DANE的目标域分类为“伪造”。

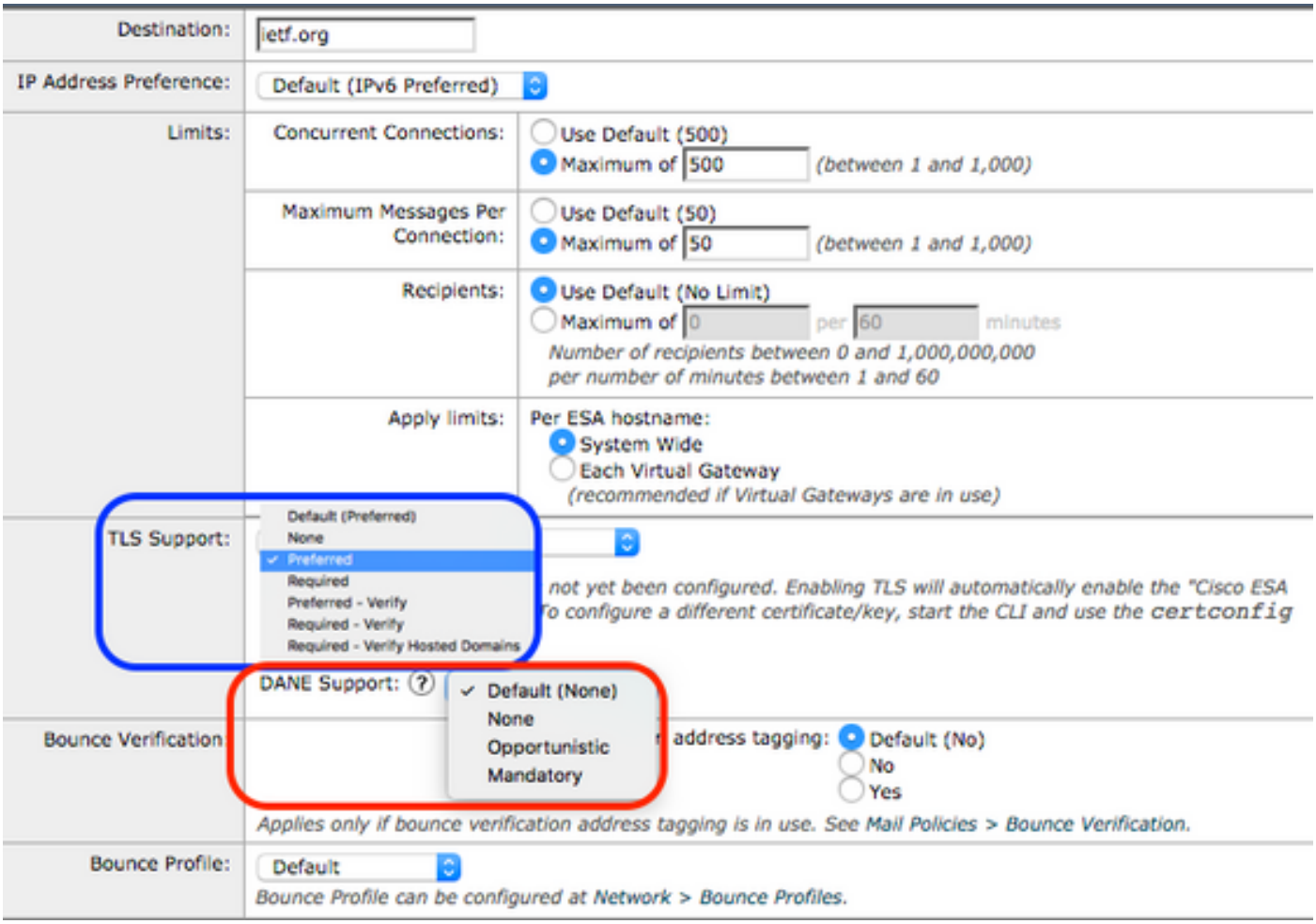
管理辅助DNS服务器

当DNS解析器无法访问时，DNS将回退到辅助DNS服务器。如果未在辅助DNS服务器上配置DNSSEC，则支持DANE的目标域的MX记录将分类为“伪造”。 这会影响消息传送，而不考虑DANE设置（“专案”或“强制”）。 思科建议您使用支持DNSSEC的辅助解析器。

配置

为出站邮件流配置DANE。

1. 网络导航到>邮件策略>目标控制>添加目标
2. 根据您的偏好完成配置文件的顶部。
3. TLS支持：**必须设置为“首选TLS” |首选 — 验证 |必填 |必需 — 验证|必需 — 验证托管域。"**
4. 启用TLS支持后，DANE支持：下拉菜单将变为活动状态。
5. **DANE支持：选项包括“无” |专案 |必填。**
6. 完成DANE支持选项后，提交并提交更改。



目标控制配置文件 — DANE验证

验证DANE成功

交货状态

监控WebUI“Delivery Status”报告，以查找可能由于DANE故障而意外生成的目标域。

在启用服务之前执行此操作，然后定期几天以确保持续成功。

ESA WebUI > Monitor > Delivery Status >检查“活动收件人”列。

邮件日志

日志级别的默认邮件日志信息级别。

邮件日志显示DANE成功协商邮件的非常微妙的指示。

最终的出站TLS协商将包括稍微修改的输出，以在日志条目末尾包含域。

日志条目将包括“TLS成功协议”，后跟TLS版本/密码“for domain.com”。

魔力在“for”中：

```
myesa.local> grep "TLS success.*for" mail_logs

Tue Feb  5 13:20:03 2019 Info: DCID 2322371 TLS success protocol TLSv1.2 cipher DHE-RSA-AES256-
GCM-SHA384 for karakun.com
```

邮件日志调试

调试级别的自定义邮件日志将显示完整的DANE和dnssec查找、预期协商、检查的哪些通过/失败部分和成功指示器。

> **注意：为调试级别日志记录配置的邮件日志可能会消耗ESA上的额外资源，具体取决于系统负载和配置。**

为调试级别日志记录配置的邮件日志可能会消耗ESA上的额外资源，具体取决于系统负载和配置。

邮件日志通常在调试级别维护一段较长的时间。

调试级别日志可能会在短时间内生成大量邮件日志。

通常的做法是为mail_logs_d创建额外的日志订阅并设置DEBUG日志记录。

此操作可防止对现有mail_logs的影响，并允许对为订阅维护的日志量进行操作。

要控制创建的日志数量，请将要维护的文件数量限制为较小的数量，例如2-4个文件。

监控、试用期或故障排除完成后，请禁用日志。

为调试级别设置的邮件日志显示非常详细的DANE输出：

Success sample daneverify

```
daneverify ietf.org

SECURE MX record(mail.ietf.org) found for ietf.org
SECURE A record (4.31.198.44) found for MX(mail.ietf.org) in ietf.org
```

```
Connecting to 4.31.198.44 on port 25.
Connected to 4.31.198.44 from interface 194.191.40.74.
SECURE TLSA record found for MX(mail.ietf.org) in ietf.org
Checking TLS connection.
TLS connection established: protocol TLSv1.2, cipher DHE-RSA-AES256-GCM-SHA384.
Certificate verification successful
TLS connection succeeded ietf.org.
DANE SUCCESS for ietf.org
DANE verification completed.
```

debug level mail logs during the above 'daneverify' exeuction.
Sample output from the execution of the daneverify ietf.org will populate the dns lookups within the mail logs

```
Mon Feb 4 20:08:47 2019 Debug: DNS query: Q('ietf.org', 'MX')
Mon Feb 4 20:08:47 2019 Debug: DNS query: QN('ietf.org', 'MX', 'recursive_nameserver0.parent')
Mon Feb 4 20:08:47 2019 Debug: DNS query: QIP ('ietf.org','MX','194.191.40.84',60)
Mon Feb 4 20:08:47 2019 Debug: DNS query: Q ('ietf.org', 'MX', '194.191.40.84')
Mon Feb  4 20:08:48 2019 Debug: DNSSEC Response data([(0, 'mail.ietf.org.')], secure, 0, 1800)
Mon Feb 4 20:08:48 2019 Debug: DNS encache (ietf.org, MX, [(8496573380345476L, 0, 'SECURE', (0,
'mail.ietf.org'))])
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q('mail.ietf.org', 'A')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QN('mail.ietf.org', 'A',
'recursive_nameserver0.parent')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QIP ('mail.ietf.org','A','194.191.40.84',60)
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q ('mail.ietf.org', 'A', '194.191.40.84')
Mon Feb  4 20:08:48 2019 Debug: DNSSEC Response data(['4.31.198.44'], secure, 0, 1800)
Mon Feb 4 20:08:48 2019 Debug: DNS encache (mail.ietf.org, A, [(8496573380345476L, 0, 'SECURE',
'4.31.198.44')])
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q('mail.ietf.org', 'AAAA')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QN('mail.ietf.org', 'AAAA',
'recursive_nameserver0.parent')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QIP ('mail.ietf.org','AAAA','194.191.40.84',60)
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q ('mail.ietf.org', 'AAAA', '194.191.40.84')
Mon Feb 4 20:08:48 2019 Warning: Received an invalid DNSSEC Response:
DNSSEC_Error('mail.ietf.org', 'AAAA', '194.191.40.84', 'DNSSEC Error for hostname mail.ietf.org
(AAAA) while asking 194.191.40.84. Error was: Unsupported qtype') of qtype AAAA looking up
mail.ietf.org
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q('mail.ietf.org', 'CNAME')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QN('mail.ietf.org', 'CNAME',
'recursive_nameserver0.parent')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QIP ('mail.ietf.org','CNAME','194.191.40.83',60)
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q ('mail.ietf.org', 'CNAME', '194.191.40.83')
Mon Feb 4 20:08:48 2019 Debug: DNSSEC Response data([], , 0, 1800)
Mon Feb 4 20:08:48 2019 Debug: Received NODATA for domain mail.ietf.org type CNAME
Mon Feb 4 20:08:48 2019 Debug: No CNAME record(NoError) found for domain(mail.ietf.org)

Mon Feb  4 20:08:49 2019 Debug: DNS query: Q('_25._tcp.mail.ietf.org', 'TLSA')
Mon Feb 4 20:08:49 2019 Debug: DNS query: QN('_25._tcp.mail.ietf.org', 'TLSA',
'recursive_nameserver0.parent')
Mon Feb 4 20:08:49 2019 Debug: DNS query: QIP
('_25._tcp.mail.ietf.org','TLSA','194.191.40.83',60)
Mon Feb 4 20:08:49 2019 Debug: DNS query: Q ('_25._tcp.mail.ietf.org', 'TLSA', '194.191.40.83')
Mon Feb  4 20:08:49 2019 Debug: DNSSEC Response
data(['0301010c72ac70b745ac19998811b131d662c9ac69dbdbe7cb23e5b514b56664c5d3d6'], secure, 0,
1800)
Mon Feb  4 20:08:49 2019 Debug: DNS encache (_25._tcp.mail.ietf.org, TLSA, [(8496577312207991L,
0, 'SECURE', '0301010c72ac70b745ac19998811b131d662c9ac69dbdbe7cb23e5b514b56664c5d3d6')])
```

fail sample daneverify

[]> thinkbeyond.ch

INSECURE MX record(thinkbeyond-ch.mail.protection.outlook.com) found for thinkbeyond.ch
INSECURE MX record(thinkbeyond-ch.mail.protection.outlook.com) found. The command will still proceed.
INSECURE A record (104.47.9.36) found for MX(thinkbeyond-ch.mail.protection.outlook.com) in thinkbeyond.ch
Trying next A record (104.47.10.36) for MX(thinkbeyond-ch.mail.protection.outlook.com) in thinkbeyond.ch
INSECURE A record (104.47.10.36) found for MX(thinkbeyond-ch.mail.protection.outlook.com) in thinkbeyond.ch
DANE FAILED for thinkbeyond.ch
DANE verification completed.

mail_logs

Sample output from the execution of he danverify thinkbeyond.ch will populate the dns lookups within the mail logs

```
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q('thinkbeyond.ch', 'MX')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QN('thinkbeyond.ch', 'MX',
'recursive_nameserver0.parent')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QIP ('thinkbeyond.ch','MX','194.191.40.84',60)
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q ('thinkbeyond.ch', 'MX', '194.191.40.84')
Mon Feb  4 20:15:52 2019 Debug: DNSSEC Response data([(10, 'thinkbeyond-
ch.mail.protection.outlook.com.')], insecure, 0, 3600)
Mon Feb 4 20:15:52 2019 Debug: DNS encache (thinkbeyond.ch, MX, [(8502120882844461L, 0,
'INSECURE', (10, 'thinkbeyond-ch.mail.protection.outlook.com'))])
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q('thinkbeyond-ch.mail.protection.outlook.com', 'A')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QN('thinkbeyond-ch.mail.protection.outlook.com', 'A',
'recursive_nameserver0.parent')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QIP ('thinkbeyond-
ch.mail.protection.outlook.com','A','194.191.40.83',60)
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q ('thinkbeyond-ch.mail.protection.outlook.com', 'A',
'194.191.40.83')
Mon Feb  4 20:15:52 2019 Debug: DNSSEC Response data(['104.47.9.36', '104.47.10.36'], insecure,
0, 10)
Mon Feb 4 20:15:52 2019 Debug: DNS encache (thinkbeyond-ch.mail.protection.outlook.com, A,
[(8497631700844461L, 0, 'INSECURE', '104.47.9.36'), (8497631700844461L, 0, 'INSECURE',
'104.47.10.36')])
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q('thinkbeyond-ch.mail.protection.outlook.com',
'AAAA')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QN('thinkbeyond-ch.mail.protection.outlook.com',
'AAAA', 'recursive_nameserver0.parent')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QIP ('thinkbeyond-
ch.mail.protection.outlook.com','AAAA','194.191.40.84',60)
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q ('thinkbeyond-ch.mail.protection.outlook.com',
'AAAA', '194.191.40.84')
Mon Feb 4 20:15:52 2019 Debug: DNSSEC Response data([], , 0, 32768)
Mon Feb 4 20:15:52 2019 Debug: Received NODATA for domain thinkbeyond-
ch.mail.protection.outlook.com type AAAA
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q('thinkbeyond-ch.mail.protection.outlook.com',
'CNAME')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QN('thinkbeyond-ch.mail.protection.outlook.com',
'CNAME', 'recursive_nameserver0.parent')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QIP ('thinkbeyond-
ch.mail.protection.outlook.com','CNAME','194.191.40.83',60)
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q ('thinkbeyond-ch.mail.protection.outlook.com',
'CNAME', '194.191.40.83')
Mon Feb 4 20:15:53 2019 Warning: Received an invalid DNS Response: SERVER FAILED to IP
194.191.40.83 looking up thinkbeyond-ch.mail.protection.outlook.com
Mon Feb 4 20:15:53 2019 Debug: DNS query: QIP ('thinkbeyond-
ch.mail.protection.outlook.com','CNAME','194.191.40.84',60)
Mon Feb 4 20:15:53 2019 Debug: DNS query: Q ('thinkbeyond-ch.mail.protection.outlook.com',
'CNAME', '194.191.40.84')
Mon Feb 4 20:15:54 2019 Warning: Received an invalid DNS Response: SERVER FAILED to IP
194.191.40.84 looking up thinkbeyond-ch.mail.protection.outlook.com
Mon Feb 4 20:15:54 2019 Debug: No CNAME record() found for domain(thinkbeyond-
ch.mail.protection.outlook.com)
```

相关信息

- ESA用户指南
- ESA版本说明
- ESA CLI参考指南